AMENDMENTS TO THE CLAIMS

Amendments to the Claims:

This listing of the claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method including steps of

providing a system including a playback device;

sending to a device, via a transport technique not including the playback device, a text-based activation code that includes data from which rights information is verifiable by the system;

enforcing the rights information on the system in response to the text-based activation code, [[;]] wherein the enforcing includes:

repeating:

constructing a license using license parameters available to the playback system, not using the text-based activation code;

~~cryptographically verifying at the device issuance of the license parameters by a trusted license server using at least part of the text-based activation code~~

authenticating the constructed license using at least part of the text-based activation code as a cryptographic signature;

checking that the cryptographic signature is a valid signature using a trusted license server;

selecting a different set of license parameters if the cryptographic signature is not valid;

until the cryptographic signature is determined to be a valid signature for the constructed license, wherein the valid signature and the constructed license constitute a whole license;

launching content associated with the whole license in accordance with the license parameters.

2. (Previously Presented) A method as in claim 1, including steps of ensuring that only authorized content is executed or presented by the playback device or a secure processor, or by both in combination or conjunction.

3. (Previously Presented) A method as in claim 1, including steps of sending content to the playback device using a communication link not used by the steps of sending a text-based activation code.

4. (Original) A method as in claim 1, wherein the steps of enforcing are performed at least in part by the playback device or a secure processor coupled thereto.

5. (Original) A method as in claim 1, wherein the steps of enforcing are performed by mandatory security hardware or mandatory security software.

6. (Previously Presented) A method as in claim 1, wherein the steps of enforcing include steps of decrypting at least some information derivable from the text-based activation code.

7. (Previously Presented) A method as in claim 1, wherein the steps of enforcing includes using a key derived from the activation code for decrypting a license or content.

8. (Previously Presented) A method as in claim 1, wherein the steps of enforcing includes

putting together at least an identity of the playback device and an identity of content;

applying at least part of the message, the identity of the playback device, and the identity of the content to authenticate the execution rights for the playback device for the content.

9. (Previously Presented) A method as in claim 1, wherein the steps of enforcing includes applying a key derived from the activation code as an authentication code.

10. (Previously Presented) A method as in claim 1, wherein the activation code is composed on an SMS.

11. (Previously Presented) A method as in claim 1, wherein at least a portion of the activation code is manually entered into the playback device.

12. (Previously Presented) A method as in claim 1, wherein at least a portion of the activation code is provided to the playback device, wherein the playback device processes the portion of the activation code and produces a licensing message suitable to be sent by the device, and wherein the licensing message is provided to the device.

13. (Previously Presented) A method as in claim 12, wherein the licensing message is encrypted or cryptographically authenticated by the device and sent to a license server.

14. (Previously Presented) A method as in claim 1, wherein the steps of enforcing include steps of using a decryption key available to the playback device or a secure processor coupled thereto.

15. (Previously Presented) A method as in claim 1, wherein said text-based activation code is included in a first message, further comprising:

sending a second message from the device to a license server;

sending the first message from the license server to the device, the first message including human-readable characters;

manually entering those characters to an input element coupled to the playback device.

16. (Original) A method as in claim 1, wherein the system includes a closed content distribution system capable of delivering content to the playback device using a second transport technique not including that used by the steps of sending a text-based message.

17. (Original) A method as in claim 1, wherein the system includes a closed content distribution system capable of ensuring that only authorized content is presented by the playback device or executed by the secure processor.

18. (Previously Presented) A method as in claim 1, wherein the system includes a secure processor capable of authenticating content coupled to the playback device in response to the authentication code.

19. (Previously Presented) A method as in claim 1, including steps of authenticating the rights information by the playback device or a secure processor coupled thereto.

20. (Previously Presented) A method as in claim 1, further comprising decrypting at least some information derivable from the text-based activation code.

21. (Previously Presented) A method as in claim 1, further comprising using a decryption key available to the playback device or a secure processor coupled thereto to authenticate the rights information.

22. (Canceled)

23. (Canceled)

24. (Canceled)

25. (Currently Amended) A method comprising:

providing a text-based activation code of a sufficiently small size that is convenient for a human to enter via an SMS technique;

sending the text-based activation code in a text-based message to a hand-held device using an SMS technique, the text-based activation code including information from which rights information is verifiable by a system including a playback device;

putting together, at the playback device, at least an identity of the playback device and an identity of content;

applying at least part of the message, the identity of the playback device, and the identity of the content to authenticate the execution rights for the playback device for the content, wherein the text-based activation code is not used to authenticate the execution rights;

verifying the execution rights using at least part of the text-based activation code as a cryptographic signature;

launching, when the execution rights are verified, content on the playback device in accordance with the execution rights.

26. (Previously Presented) A method as in claim 25, wherein the playback device includes at least one of rights-enforcing hardware, rights-enforcing software, further including:

authenticating the rights information using the rights-enforcing hardware or rights-enforcing software;

enforcing the rights information on the system using the rights enforcing hardware or rights enforcing software, in response to the text-based activation code.

27. (Currently Amended) A method including steps of

providing a system including a secure processor and a playback device under control of the secure processor;

sending a text-based message including an activation code to a hand-held device using an SMS technique, the activation code including information from which rights information is verifiable;

~~using the activation code to cryptographically verify rights information;~~

authenticating ~~that~~ the rights information at the secure processor in response to mandatory security software executed by the secure processor;

using the activation code as a cryptographic signature to cryptographically verify rights information;

enforcing, using the mandatory security software, the rights information on the system in response to that text-based message;

wherein the enforcing includes constructing a license using information available to the playback system, not using the activation code.

28. (Original) A method as in claim 27, including steps of sending content to the playback device using a communication link not used by the steps of sending a text-based message.

29. (Original) A method as in claim 27, wherein the steps of sending a text-based message include a transport technique not including the playback device.

30. (Original) A method as in claim 27, wherein the steps of sending a text-based message include steps of

sending a first message from a hand-held device using an SMS technique to a license server;

sending a second message from the license server to the hand-held device, the second message including human-readable characters; and

entering those characters to an input element coupled to the secure processor.

31. (Original) A method as in claim 27, wherein the system includes a closed content distribution system capable of delivering content to the playback device using a second transport technique not including that used by the steps of sending a text-based message, the closed content distribution system including the mandatory security software being responsive to a private key in a public-key cryptosystem.

32. (Original) A method as in claim 27, wherein the system includes a closed content distribution system capable of ensuring that only authorized content is presented by the playback device or executed by the secure processor.

33. (Previously Presented) A method as in claim 27, wherein

the text-based message includes an authentication code; and

the system includes a secure processor capable of authenticating content coupled to the playback device in response to the activation code.

34. (Currently Amended) A method comprising

providing a system including a playback device under control of a secure processor;

sending to a hand-held device using an SMS technique a signature over a token including a playback device identity and content identity;

providing the signature to the playback device identified in the token;

constructing a license using information available to the playback system, not using the signature;

authenticating the license using the signature;

enforcing, using security software at the playback device, a check against the playback device and the content identified in the token~~;~~

~~wherein the enforcing includes constructing a license using information available to the playback system, not using the signature~~.

35. (Currently Amended) A method comprising

providing a system including a playback device under control of a secure processor;

sending a text-based message including an activation code to a hand-held device using an SMS technique, the activation code including information from which rights information is verifiable by the system;

providing a signature associated with the activation code to the secure processor;

constructing a license using an identity of the playback device and not using the signature;

enforcing the rights information at the secure processor using the signature and the license ~~an identity of the playback device;~~

~~wherein the enforcing includes constructing a license using information available to the system, not using the activation code~~.

36. (Previously Presented) A method comprising:

providing, in a closed content distribution system, an SMS text message that includes license information in the form of an activation code that is small enough for a human to conveniently enter, the closed content distribution system including a playback device and a secure processor, wherein the SMS message is sent via a communication link not including the playback device or secure processor;

constructing, at the playback device, license parameters including a device ID, a content ID, and a rights code identified by the activation code;

using at least part of the SMS text message as a signature to authenticate the constructed license parameters;

allowing content identified by the content ID to be executed or presented by the playback device or the secure processor, or by both in combination or conjunction in accordance with the constructed and authenticated license parameters, wherein the playback device or the secure processor, or both in combination or conjunction, are associated with the device ID;

ensuring that rights information associated with the rights code is enforced by the playback device or the secure processor, or by both in combination or conjunction.

37. (Original) A method as in claim 36, including steps of authenticating the license information by the playback device or the secure processor, or by both in combination or conjunction.

38. (Original) A method as in claim 36, including steps of determining in response to the rights information whether the user is authorized to execute or present the selected content.

39. (Original) A method as in claim 36, including steps of encoding the license information using a digital signature, secure hash, or shared secret; and

authenticating the license information by the playback device or the secure processor, or by both in combination or conjunction, in response to the digital signature, secure hash, or shared secret.

40. (Original) A method as in claim 36, including steps of receiving content at the playback device.

41. (Original) A method as in claim 36, wherein at least a portion of the content is ~~12~~ included on physical media transported to the playback device or secure processor.

42. (Original) A method as in claim 36, wherein at least a portion of the content is present at the playback device or secure processor before the steps of delivering license information.

43. (Original) A method as in claim 36, wherein the communication link includes a cellular telephone.

44. (Original) A method as in claim 36, wherein the content can be executed or interpreted by the playback device or the secure processor, or by both in combination or conjunction.

45. (Original) A method as in claim 36, wherein the content can be presented in a human-sensible form by the playback device or the secure processor, or by both in combination or conjunction.

46. (Original) A method as in claim 36, wherein the secure processor includes a computing device capable of enforcing mandatory execution of selected security software.

47. (Original) A method as in claim 36, wherein the secure processor includes a 14 computing device capable of general purpose processing.

48. (Previously Presented) A method as in claim 36, wherein the steps of providing include steps of sending a text-based message to a hand-held device using an SMS technique, the text-based message including information from which rights information is derivable.

49. (Original) A method as in claim 36, wherein the steps of ensuring include steps of decoding the license information;

generating at least a portion of the rights information in response to the steps of decoding; and

enforcing the rights information.

50. (Previously Presented) A method as in claim 36, including steps of performing a commercial transaction concurrently with communication between a license server and a user.

51. (Original) A method as in claim 50, wherein the steps of performing a commercial transaction include steps of receiving information at the license server sufficient to allow that license server to effect a purchase transaction by the user.

52. (Original) A method as in claim 50, wherein the steps of performing a commercial transaction include steps of receiving proof of purchase at the license server of a license by the user.

53. (Original) A method as in claim 36, including steps of performing mandatory security software by the secure processor.

54. (Original) A method as in claim 53, wherein the steps of performing mandatory security software include one or more of:

authenticating at least one of: a specific content element, a specific playback device or secure processor, a specific user;

enforcing comparison of an identity associated with the playback device with a tamper-proof identity available to the playback device or the secure processor, or to both in combination or conjunction;

enforcing comparison of rights information with an identity of selected content available to the playback-device or the secure processor, or to both in combination or conjunction;

enforcing computation of the secret key (using its private key and server public key) and decryption of the identities; and

enforcing verification of a signature by the license server.

55. (Previously Presented) A method as in claim 36, wherein the steps of providing include steps of delivering the activation code from a license server to a user; and

manually communicating the activation code from the user to the playback device or the secure processor.

56. (Previously Presented) A method as in claim 55, including steps of deriving license information from the activation code.

57. (Previously Presented) A method as in claim 55, including steps of decrypting content in response to the activation code.

58. (Previously Presented) A method as in claim 55, wherein the activation code includes a human-readable alphabetic, alphanumeric, numeric, or other character string.

59. (Previously Presented) A method as in claim 55, wherein the activation code includes a representation of at least a portion of a license message.

60. (Previously Presented) A method as in claim 55, wherein the steps of communicating the activation code include a human input device.

61. (Previously Presented) A method as in claim 55, wherein the steps of communicating the activation code include an input technique not part of the closed distribution system.

62. (Previously Presented) A method as in claim 55, wherein the steps of communicating the activation code include an SMS protocol.

63. (Previously Presented) A method as in claim 55, wherein the steps of communicating the activation code include a text messaging protocol.

64. (Previously Presented) A method as in claim 55, wherein the activation code includes a representation of a content decryption key.

65. (Original) A method as in claim 64, wherein the closed distribution system includes a public-key cryptosystem; and

the content decryption key includes a decryption key privately associated with the content, encrypted by an encryption key publicly associated with a specific playback device.

66. (Canceled)

67. (Canceled)

68. (Canceled)

69. (Currently Amended) A system comprising:

a closed content distribution system including a playback device and a secure processor;

a communication link not including the playback device or secure processor;

a license server capable of being coupled to the communication link;

wherein the playback device or the secure processor, or both in combination or conjunction, includes mandatory security software that is capable of verifying rights information associated with a license from a text-based activation code received on the communication link, wherein license parameters of the license do not include the text-based activation code, and wherein the text-based activation code includes a signature used to cryptographically verify the license.

70. (Original) Apparatus as in claim 69, wherein at least a portion of the content is included on physical media transported to the playback device or secure processor.

71. (Original) Apparatus as in claim 69, wherein the communication link includes a cellular telephone.

72. (Original) Apparatus as in claim 69, wherein the mandatory security software includes instructions authenticating the license information.

73. (Original) Apparatus as in claim 69, wherein the mandatory security software includes instructions determining in response to the rights information whether the user is authorized to execute or present the selected content.

74. (Previously Presented) Apparatus as in claim 69, wherein the mandatory security software includes instructions of

encoding the license information using a digital signature, secure hash, or shared secret; and

authenticating the license information by the playback device or the secure processor, or by both in combination or conjunction, in response to the digital signature, secure hash, or shared secret.

75. (Original) Apparatus as in claim 69, wherein

the mandatory security software includes instructions ensuring that only authorized content is executed or presented by playback device or the secure processor, or both in combination or conjunction; and

rights information derivable from the license information is enforced by the playback device or the secure processor, or by both in combination or conjunction.

76. (Original) Apparatus as in claim 69, wherein the mandatory security software includes one or more of:

instructions authenticating at least one of: a specific content element, a specific playback device or secure processor, and a specific user;

instructions enforcing comparison of an identity associated with the playback device with a tamper-proof identity available to the playback device or the secure processor, or to both in combination or conjunction;

instructions enforcing comparison of rights information with an identity of selected content available to the playback device or the secure processor, or to both in combination or conjunction;

instructions enforcing computation of the secret key (using its private key and server public key) and decryption of the identities; and

instructions enforcing verification of a signature by the license server.

77. (Original) Apparatus as in claim 69, wherein the secure processor includes a computing device capable of general purpose processing.

78. (Original) Apparatus as in claim 69, including a code delivered from a license server to a user, the code being communicated from the user to the playback device or the secure processor.

79. (Original) Apparatus as in claim 78, including a content decryption key embedded in the code.

80. (Original) Apparatus as in claim 78, including a human input device coupled to the playback device or the secure processor.

81. (Original) Apparatus as in claim 78, including license information embedded in the code.

82. (Original) Apparatus as in claim 78, including an SMS protocol message.

83. (Original) Apparatus as in claim 78, including a text messaging protocol message.

84. (Original) Apparatus as in claim 78, wherein the code includes a human-readable alphabetic, alphanumeric, numeric, or other character string.

85. (Canceled)

86. (Original) Apparatus as in claim 78, wherein the code includes a representation of a content decryption key.

87. (Original) Apparatus as in claim 86, wherein

the closed distribution system includes a public-key cryptosystem; and

the content decryption key includes a decryption key privately associated with the content, encrypted by an encryption key publicly associated with a specific playback device.

88. (Canceled)

89. (Previously Presented) Apparatus as in claim 69, wherein the mandatory security software includes instructions authenticating the code, the instructions including one or more of:

instructions determining if the code is digitally signed by a license server; and

instructions determining if the code is encrypted by a key known commonly to both the license server and the specific user.

90. (Previously Presented) Apparatus as in claim 69, wherein the mandatory security software includes instructions authenticating the code, the instructions including one or more of:

instructions determining if the code is digitally signed by a license server; and

instructions determining if the code is encrypted by a key known commonly to both the license server and the specific playback device or secure processor, or both in combination or conjunction.

91. (Previously Presented) A method as in claim 1, further comprising:

constructing parameters of execution rights for the hand-held device or the content;

providing a system including a playback device;

sending to the playback device, via a transport technique not including the playback device, a text-based message associated with an SMS technique, wherein the text-based message is derivable by the system;

enforcing, using mandatory security hardware or mandatory security software, the rights information on the system in response to the text-based message, said enforcing including:

constructing parameters of execution rights for the playback device;

using at least part of the text-based message as a signature to authenticate the execution rights.

92. (Previously Presented) A method as in claim 1, wherein the cryptographically verifying includes using at least part of the activation code as a cryptographic signature generated using a private key of a public key cryptographic key pair.

93. (Previously Presented) A method as in claim 1, wherein the cryptographically verifying includes computing a cryptographic signature using a computed shared secret key to construct a message authentication code (MAC).

94. (Previously Presented) A method as in claim 1, wherein the cryptographically verifying includes decrypting the activation code using a computed shared secret key and matching the decrypted activation code against the license parameters.

95. (Previously Presented) A method as in claim 1, wherein one or more of the license parameters are selected from the group consisting of: a device identity, a content identity, and a rights code.

96. (Previously Presented) A method as in claim 27, further comprising using at least part of the activation code as a cryptographic signature generated using a private key of a public key cryptographic key pair.

97. (Previously Presented) A method as in claim 27, further comprising:

using at least part of the activation code as an encrypted message from a license server;

decrypting said encrypted message using a shared secret key computed by the playback device;

verifying that the decrypted message verifies against said constructed license.